MARYLAND DEPARTMENT OF JUVENILE SERVICES

POLICY & PROCEDURE

SUBJECT: **Virtual Private Network (VPN) Policy**
NUMBER: **IT-02-08 (Information Technology)**
APPLICABLE TO: **DJS Information Technology Unit and Users of the VPN Service**
EFFECTIVE DATE: **June 6, 2008**

Approved: "/s/signature on original copy"
Donald W. DeVore, Secretary

1. POLICY. The Department of Juvenile Services (DJS) establishes this policy to provide guidelines for remote access to the DJS network, data, and applications. The Department's network shall be accessed when performing official job functions which are not accessible through the DJS website and the employee is working from a remote location.

2. AUTHORITY.

a. State of Maryland Department of Budget and Management - Information Technology Security Policy and Standards – Version 1.5 (January 2007).
b. Annotated Code of Maryland State Personnel and Pension, Article §4-103.

3. DEFINITIONS.

a. *Chief Information Officer* means the individual responsible for managing the Information Technology Unit.
b. *Executive Staff* means high level DJS personnel which includes the Secretary, Deputy Secretary, Assistant Secretary, Principal Counsel and positions designated by the Secretary.
c. *Official DJS Business* means use that is directly related to the operation of DJS.
d. *Virtual Private Network* means a computer network that uses a public network such as the internet to transmit private data.

4. PROCEDURES.

a. General Procedures.

(1) Executive staff and approved employees may utilize the benefits of the Virtual Private Network (VPN) service.

(2) VPN users are responsible for selecting an Internet Service Provider (ISP) with broadband service and the payment of the associated costs. Dial-up service will not be supported by DJS Information Technology (IT).

(3) VPN users must be assigned DJS equipment which is configured with the proper security software to access the DJS network remotely.

(4) DJS equipment shall be used to access to VPN.

(5) VPN shall not be used for purposes other than official DJS Business.

b. Request, Approval, and Denial Process.

(1) VPN access must be requested by the employee's supervisor by submitting an IT System Access Request Form along with a signed VPN Policy Receipt Form to the DJS IT Help Desk. The IT System Access Request Form must include a justification as to why the user needs VPN access.

(2) Once approved by the Chief Information Officer (CIO) or designee, the access is set up by a Network Administrator.

(3) The Network Administrator (or designee) will notify the supervisor by email when the access is approved and available and/or denied.

(4) Requests shall be denied for the following reasons:

(i) Incomplete forms will be returned to the supervisor with a request to provide the missing information;
(ii) Requests submitted without a signed VPN Policy Receipt form will not be processed until the form is received; and
(iii) Justification does not meet criteria for VPN access.

c. VPN Users Responsibilities.

(1) Selecting an Internet Service Provider (ISP) that provides broadband service and paying associated costs.

(2) Acquiring a computer that has been configured by the IT Unit that will allow proper connection to the DJS network.

(3) Ensuring that unauthorized users are not logging onto the DJS internal networks or viewing confidential data.

(4) Keeping their account active. If the account hasn't been used for 60 days, it will be removed. To regain VPN access, the initial request procedure must be followed.

(5) Ensuring VPN session is active. VPN connection will be disconnected if left idle for 15 minutes, requiring the user to reconnect.

(6) Notifying the IT Unit when VPN access is no longer needed. An IT Change Request form must be completed by the supervisor indicating the access is no longer needed and e-mail the form to the IT Help Desk.

(7) Ensuring the equipment is properly maintained, and safeguarded from theft, loss, and damage.

(8) Returning all equipment issued for VPN access to the IT Unit.

d. Information Technology Responsibilities.

(1) Providing the equipment for VPN access.

(2) Configuring the equipment with the current client, application software and virus protection.

(3) Providing support and training for authorized VPN users.

(4) Monitoring VPN usage to assure that access is being managed according to policy.

(5) Removing an account that has not been used for 60 days.

e. VPN Configuration Standard.

(1) A connection that is left idle for 15 minutes will be disconnected which will force the user to reconnect.

(2) An active connection to the VPN session will force all traffic to and from the PC over the VPN tunnel.

(3) VPN access must meet State IT Security Standards pertaining to password security.

5. DIRECTIVES/POLICIES AFFECTED.

a. Directives/Policies Rescinded - **None**

b. Directives Referenced - **None.**

6. LOCAL IMPLEMENTING PROCEDURES REQUIRED. No.

7. FAILURE TO COMPLY.

Failure to comply with a Secretary's Policy and Procedure shall be grounds for disciplinary action up to and including termination of employment.

Appendix – None.

MARYLAND DEPARTMENT OF JUVENILE SERVICES
EMPLOYEE STATEMENT OF RECEIPT
POLICY AND PROCEDURE

SUBJECT: Virtual Private Network (VPN) Policy
POLICY NUMBER: IT-02-08 (Information Technology)
EFFECTIVE DATE: June 6, 2008

I have received one copy (electronic or paper) of the Policy and/or Procedure as titled above. I acknowledge that I have read and understand the document, and agree to comply with it.

_____ _____
SIGNATURE PRINTED NAME

_____
DATE

(THE ORIGINAL COPY MUST BE RETURNED TO YOUR IMMEDIATE SUPERVISOR FOR FILING WITH PERSONNEL, AS APPROPRIATE.)